IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

HAYWARD INDUSTRIES, INC.,	:	Civil Action No. 3:20-CV-710 -MOC-DSC
Plaintiff(s), Counterclaim Defendant	:	
v.	:	
BLUEWORKS CORPORATION, BLUEWORKS INNOVATION CORPORATION, NINGBO C.F. ELECTRONIC TECH CO., LTD; NINGBO YISHANG IMPORT AND EXPORT CO., LTD.	:	
Defendant(s).	:	

DECLARATION OF XIONG (CARL) LI IN SUPPORT OF PLAINTIFF'S REPLY IN SUPPORT OF MOTION TO COMPEL

I, Xiong (Carl) Li, hereby declare as follows:

1. I am a licensed attorney practicing with Zhong Lun Law Firm, Shanghai Office. I have been practicing law in China for more than twenty years. I submit this declaration in support of Plaintiff's Reply in Support of Motion to Compel, filed herewith.

2. I have been asked to provide a legal opinion regarding Defendants' Opposition to Motion to Compel. I understand that Hayward Industries, Inc. ("Hayward") has obtained a judgment in excess of $16,000,000 against Defendants Blueworks Innovation Corporation, Ningbo C.F. Electronic Tech Co., Ltd., and Ningbo Yishang Import and Expert Co., Ltd. After obtaining its judgment, Hayward served the First Set of Post Judgment Discovery to Ningbo C.F. Electronic Tech Co., Ltd., the First Set of Post Judgment Discovery to Ningbo Yishang Import and Export Co., Ltd., and the First Set of Post Judgment Discovery to Blueworks Innovation Corporation (collectively, the "Requests"). I have reviewed each set of post judgment discovery requests along with Hayward's Memorandum in Support of Motion to Compel Non-Debtor Defendants to Respond to Post-Judgment Discovery Requests, Defendants' Response in Opposition to Hayward's Motion to Compel Non-Debtor Defendants to Response to Post-Judgment Discovery Request, and the Declaration of Qian Hang in Support of Defendants' Opposition to Plaintiff Hayward Industries, Inc.' Motion to Compel. A true and accurate copy of

those documents is attached to this Declaration as Exhibits A, B, C, D, E, and F.

3. I understand from the Declaration of Quian Hang that Mr. Hang is an attorney that has represented both Ningbo co-defendants in prior matters, including Ningbo "C.F." Electronic Tech. Co. Ltd., because the word "Sihu" used in his Declaration is a Chinese pronunciation for "C.F." I have been outside counsel in prior matters to Hayward Industries (Wuxi) Co. Ltd, which is a Chinese subsidiary of Hayward.

4. Based on my review of the Requests, Defendants' Opposition, and the relevant Chinese legal authorities, it is my professional opinion, to a reasonable degree of legal certainty, that the laws and regulations of the People's Republic of China do not preclude the Defendants from providing the data and information sought by Hayward in the Requests. Further, the laws and regulations cited by Defendants in their Opposition and in the Declaration of Qian Hang do not preclude them from providing the data and information requested by Hayward in the Requests. I summarize my analysis as well as the relevant laws in China below.

Law of the People's Republic of China on Guarding State Secrets

5. Articles 27 and 28 of *Law of the People's Republic of China on Guarding State Secrets* ("State Secrets Law") cited by Defendant's Chinese legal expert are only applicable if the data or information disclosed fall within the category of "State Secrets". None of the information or data sought by the Requests qualifies as a State Secret of the People's Republic of China. Therefore, the State Secrets Law does not prevent Defendants from responding to the Requests and producing the requested data and information.

6. Article 13 of the State Secrets Law delineates a precise definition of "State Secrets", as included below:

> "*The following matters involving national security and interests, which may harm the security and interests of the country in political, economic, national defense, diplomatic and other fields if leaked, shall be determined as "State Secret":*
> *(i) secret matters in major national decision-making processes;*
> *(ii) secret matters in national defense construction and armed forces activities;*
> *(iii) secret matters in diplomatic and foreign affairs activities, as well as secrets subject to confidentiality obligations in foreign engagements;*
> *(iv) secret matters in the national economy and social development;*
> *(v) secret matters in scientific and technological fields;*
> *(vi) secret matters in activities to maintain national security and to investigate criminal offenses;*
> *(vii) other secret matters determined by the national administration for secrecy.*
> *Matters that are secrets of political parties and meet the provisions of the preceding paragraph are State Secret.*".

7. Based on my experience, data or information that implicates State Secret is

generally connected with government bodies, public institutions, state-owned companies, and pivotal industries including defense, infrastructure, transportation, and water resources. Because the Defendants are private manufactures of swimming pool products, their data does not contain State Secrets. Consequently, the State Secrets Law does not apply to prevent them from responding to the Requests and producing the data and information requested therein.

Data Security Law of the People's Republic of China

8. The Defendants claim that the *Data Security Law of the People's Republic of China* ("Data Security Law") prevents them from responding to the Requests. This claim is incorrect because the information sought in the Requests is classified under the Data Security Law as "General Data." The Data Security Law does not require that any approval be obtained from Chinese governmental authorities before the production of General Data.

9. The Data Security Law is formulated to regulate data processing activities, ensure data security, promote the development and utilization of data, protect the legitimate rights and interests of individuals and organizations, and safeguard national sovereignty, security, and development interests.

10. According to the Article 21 of Data Security Law, China has established a data classification and grading protection system based on the importance of data in economic and social development, as well as the degree of harm that may be caused to national security, public interest, or the legitimate rights and interests of individuals and organizations. Although Data Security Law mentioned concept of "Important Data" and "Core Data" when it was published in 2021, the concepts were undefined and were left to relevant authorities to classify.

11. Subsequently, The State Administration for Market Regulation and the Standardization Administration of China issued the *Data Security Technology - Rules for Data Classification and Grading* (GB/T 43697-2024) on March 15, 2024, which classified data into three categories: "Core Data", "Important Data", and "General Data". Specifically:

- **"Core Data"** refers to Important Data that has a high coverage or reaches a high degree of accuracy, scale, or depth for a field, group, or region, and may directly affect political security if illegally used or shared.
- **"Important Data"** refers to data that is specific to a field, group, region, or reaches a certain degree of accuracy and scale, and may directly endanger national security, economic operation, social stability, public health, and safety if it is leaked, tampered with, or destroyed (data that only affects the organization itself or individual citizens is generally not considered important data).
- **"General Data"** refers to all other data that is not classified as Core Data or Important Data.

12. Based on the above definition, the data requested in Plaintiff's Post-judgment Discovery Request is only related to the Defendants' company asset clues and does not involve

Important Data (let alone Core Data) that could endanger national security, economic operation, social stability, public health, and safety. The data requested by Plaintiff falls under the category of General Data without any doubt.

13. In addition, Article 21 of Data Security Law stipulates that '*all regions and departments shall, under the data classification and hierarchical protection system, determine the specific catalogue of important data for their respective regions and departments and for relevant industries and fields, and give priority to the protection of data included in the catalogue*'. Ningbo City (or even broader, Zhejiang Province), where the Defendants are located, has not issued any specific catalog of important data, which further confirms that the data requested in Plaintiff's Post-judgment Discovery Request does not belong to Core Data or Important Data.

14. The Defendants' Chinese expert quoted Article 36 of the Data Security Law and seems to indicate that Defendants are not allowed to provide data stored in China to foreign judicial or law enforcement agencies without the approval of the competent authorities in China. It is notable that based on the current practice in China, "approval of the competent authority" refers to the supervision and approval of the Cyberspace Administration of China, whose scope of supervision is currently only limited to "Important Data" among the three categories of data and certain "Personal Information" (under *Personal Information Protection Act of the People's Republic of China*, see below for detailed analysis). For General Data, the Cyberspace Administration of China does not restrict its overseas transfer and thus no approval is required.

15. In conclusion, it is my professional opinion that the information or data requested by Plaintiff in this case is only 'General Data' under Data Security Law, and Defendants' providing the information and data in this case is not subject to any approval from Chinese government authority.

Personal Information Protection Act of the People's Republic of China

16. The Defendants quoted *Personal Information Protection Act of the People's Republic of China* ("PIPL"), and suggests that the cross-border transfer of the information requested by Plaintiff shall be prohibited without approval from the competent authorities. This suggestion is incorrect because the PIPL only requires approval from the requisite authorities if the data processors that are producing the information have already provided personal information of more than 100,000 people and/or the sensitive personal information of more than 10,000 people since January 1, 2024 in one or more cross-border data transfers. Neither the Opposition nor the Declaration of Qian Hang claims that the Defendants have transferred sufficient personal information or sensitive personal information across a border so as to subject their transfer of the data and information requested in the Requests to review by the authorities. Therefore, the PIPL does not require Defendants to obtain any governmental review of their responses to the Requests prior to producing data or information to Hayward. Further, even if review would otherwise be required, it is not in this case because the PIPL contains an exception that allows data and information to be produced when the production is required by law. Because Defendants are required to respond to the Requests and produce the data and information sought therein by law,

the PIPL does not bar the Defendants from doing so.

16. Firstly, the Defendants' Chinese expert wrong cited the articles of PIPL. Article 21 cited by the Defendants' Chinese expert is from Data Security Law (mentioned in the above section). It is irrelevant to PIPL.

16. Secondly, the Defendants' Chinese expert quoted Article 31 of the PIPL and seems to indicate that Defendants are not allowed to provide personal data in China to foreign judicial or law enforcement agencies without the approval of the competent authorities in China. As mentioned in the above section, the current practice in China is that the "approval of the competent authority" refers to the supervision and approval of the Cyberspace Administration of China. However, only personal data that reaches a certain quantity threshold is subject to review from Cyberspace Administration of China. Article 4 of the *Methods for Data Export Security Assessment* (same quotation as the Defendants' Chinese expert) states that the Cyberspace Administration of China only requires a declaration of data export security assessment to the Cyberspace Administration when the data processors providing the personal information to an overseas entity have cumulatively provided personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals to overseas entities since the previous January 1st. The Requests do not seek the personal information or sensitive personal information of 10,000 individuals, and neither the Defendants nor their expert contend that the Defendants have provided either the personal information of 100,000 people or the sensitive personal information of 10,000 since January 1, 2024. Therefore, the PIPL does not require any review by any Chinese governmental authority of the information and data sought by the Requests prior to its production to Hayward.

17. In fact, the newly enacted *Regulations on Promoting and Regulating the Cross-Border Data Flow* ("New Regulation on Data Cross-Border Transfer"), Order No. 16 of the Cyberspace Administration of China, which came into effect on March 22, 2024, significantly eases the constraints on the transfer of data across borders. Specifically, Article 5 of the New Regulation on Data Cross-Border Transfer provides a list of scenarios that are exempted from the necessity of undergoing an approval process or fulfilling other compliance requirements when providing data or information to entities located outside of China.

> "*Article 5: data processors who provide personal information to overseas entities under one of the following scenarios are exempt from declaring a data export security assessment, entering into a standard contract for personal information export, or passing personal information protection certification: ...(iv) For data processors other than operators of critical information infrastructure, who have provided personal information to overseas entities for less than 100,000 people since January 1 of the current year (excluding sensitive personal information)...* "

18. In this case, the information requested by Hayward is far less than the threshold and Defendants are not obligated to take any act under the PIPL to cause the Chinese governmental authorities to review their responses to the Requests prior to producing data and

information to Hayward.

19. Thirdly, Article 13 of PIPL states "*under any of the following circumstances may a personal information handler handle personal information: ...(3) where it is necessary for the performance of duties or obligations provided by law;...*" In other words, PIPL Article 13 allows for an exception where Defendants shall be allowed to disclose personal information if the request is pursuant to a legal obligation. Article 13(3) of PIPL does not distinguish between obligations under Chinese or foreign law. The legal obligation of Defendants under the U.S. law to respond to the Requests causes their responses to fall under Article 13's exception clause.

20. Fourthly, as far as I know, there has not been any case involving penalty of cross-border transmission of personal data upon the orders of a foreign court.

21. In conclusion, the information or data requested by Hayward in this case does not reach the quantity threshold that requires any review by the Chinese government authority under PIPL.

Cybersecurity Law of the People's Republic of China

22. *Cybersecurity Law of the People's Republic of China* ("Cybersecurity Law") is formulated to safeguard network security, maintain cyberspace security. In my opinion, Cybersecurity Law is not relevant in this case at all because it only applies to entities that are Operators of Critical Information Infrastructure. As private manufacturers of swimming pool products, Defendants do not meet the definition of Operators of Critical Information Infrastructure. Therefore, the Cybersecurity Law is inapplicable to them.

23. Defendants' Chinese expert cited Article 37 of the Cybersecurity Law, which pertains solely to the regulation of activities of "Operators of Critical Information Infrastructure". Article 2 of *Regulation on the Security Protection of Critical Information Infrastructure*, Order No. 745 of the State Council, which came into effect on September 1, 2021, delineates a precise definition of "Operator of Critical Information Infrastructure", which is "*important network facilities and information systems in key industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, electronic government affairs, and national defense science and technology industry, as well as others that, if disrupted, lose functionality, or suffer data breaches, could severely endanger national security, economic stability, and public interest*." The defendants are private companies engaged in business of manufacturing swimming pool products. The nature of Defendants business as well as the nature of their industry does not meet the definition of Operator of Critical Information Infrastructure. In addition, the number of entities that are considered as Operators of Critical Information Infrastructure in China is quite limited, and they are only considered as such when the competent authority explicitly notifies them in writing that they are Operators of Critical Information Infrastructure and requires them to comply with specific obligations. If no explicit notification is received from the competent authority, the entity does not belong to the Operator of Critical Information Infrastructure. Defendants do not even claim to have been notified that they

are an Operator of Critical Information Infrastructure.

24. The Cybersecurity Law does not preclude Defendants from responding to the Requests and producing the requested information and data.

Methods for Data Export Security Assessment

25. *Methods for Date Export Security Assessment* ("Security Assessment Method") is formulated in accordance with laws and regulations such as the Cybersecurity Law, Data Security Law, and PIPL in order to regulate cross-border data transmission activities.

26. The Article 4 of the Security Assessment Method quoted by the Defendants' Chinese legal expert's citation inadvertently substantiates our conclusion that the regulatory scope of Cyberspace Administration of China is currently confined to "Important Data" and "Personal information".

27. The data or information implicated in the Requests does not meet the conditions set forth in Article 4 of the Security Assessment Method: (a) the requested data does not constitute the Important Data as delineated in Article 4, paragraph 1, of the Security Assessment Method; (b) the Defendants are not categorized as Operators of Critical Information Infrastructure as indicated in Article 4, paragraph 2, of the Security Assessment Method; and (c) although the request encompasses a modicum of personal information, the quantity significantly falls short of the threshold of 100,000 individuals' personal information and 10,000 individuals' sensitive personal information as mandated in Article 4, paragraph 2, of the Security Assessment Method.

28. In light of the above, the Defendants' Chinese legal expert citation of Article 4 and Article 5 of the Security Assessment Method fails to establish that the Defendants are precluded by Security Assessment Method from supplying the data or information demanded by Hayward.

Civil Procedure Law of the People's Republic of China

29. Article 294, 295 and 296 of *Civil Procedure Law of the People's Republic of China* ("Civil Procedure Law") are not new contents; they were not added when Civil Procedure Law was updated in 2023. Rather, these clauses have been in Civil Procedure Law since its first version from 1991, before China joined Hague Evidence Convention.

30. Civil Procedure Law only states that actions proactively to 'collect' evidence in China shall go through relevant treaty or conventions – namely Hague Evidence Convention process. It does not prohibit a Chinese party from providing data or information to a foreign court or the opposing party.

31. In fact, there have been quite a few cases where Chinese companies are compelled by courts in the United States to provide evidence or data. As far as I know, the Chinese government has never penalized a Chinese company for providing the company's own information

or data upon the orders of a foreign court without going through the Hague Evidence Convention procedures.

Frequently Asked Questions on Interpretation Judicial Assistance in Civil and Commercial Matters

32. The Defendants' Chinese expert Qian Hang quoted a questions and answers section regarding the Civil Procedure Law about 'foreign judicial organs or personnel access evidence materials in China' and 'commission a lawyer or other institution in China to question witness or other person or access materials located in China' to suggest that Defendants may not answer the Requests. This suggestion is based upon an inaccurate translation. Mr. Hang translates the Chinese term used in the questions and answers as "access" and indicates that, as a result, foreign judicial authorities and judicial personal may not access information in China. The original Chinese word at issue is more appropriately translated into 'collect' or 'retrieve', which is the same translation used in used in the Civil Procedure Law itself. The translation of the whole section is included below.

"II Regarding Investigation and Evidence Collection

5. How can foreign judicial authorities or judicial personnel retrieve evidence materials located within China?
Answer: According to the channels stipulated in the treaty, foreign judicial organs or individuals with the qualifications to request evidence should submit investigation and evidence retrieval requests to the Ministry of Justice. If no relevant treaty has been concluded with China, a request should be made to the Ministry of Foreign Affairs. After approval, the request shall be executed by the people's court, and the result shall be replied to by the requesting department.

6. Can foreign judicial authorities or individuals directly question (including through technical means such as telephone, video, etc.) witnesses located within China?
Answer: No. When China joined the Hague Evidence Convention, it made a reservation to Chapter II of the Convention, except for Article 15, which does not allow foreign judicial authorities to directly collect evidence from witnesses located in China. Foreign relevant institutions should submit evidence collection requests to the Ministry of Justice through treaty stipulated channels or to the Ministry of Foreign Affairs through diplomatic channels. After approval, the requests will be executed by the people's court.

7. Can foreign judicial authorities or related personnel entrust lawyers or other institutions within China to question witnesses or other individuals, or retrieve materials located within China, and use the results for litigation in foreign courts?
Answer: According to the Civil Procedure Law of China, evidence collection shall be conducted by the people's court or by lawyers with the approval of the people's court. No other institution or individual may collect evidence within the territory of China."

33. As explained by the questions and answers, the purpose of this section is to prohibit investigating, collecting evidence or questioning witness proactively by 'foreign judicial authorities or personnel in China, emphasizing the integrity of the national territory. It does not, however, prevent any individual or entity in China from voluntarily providing information or documents to the opposing party or court following relevant foreign laws or regulations. In this case, the Hayward is requesting Defendants to provide evidence in a post-judgment discovery process. Plaintiff is not interrogating any witness in China, nor does the Hayward or the Court send anyone to China to collect or retrieve any evidence proactively. The quoted questions and answers do not prevent the Defendants from responding to the Requests.

Hague Evidence Convention process

34. Requests raised through Hague Evidence Convention may take a long time. According to an article published on December 4th, 2023 by People's Court Daily (a newspaper managed and issued by the Supreme Court of China), from 2008 to 2018, Chinese courts executed a total of 66 requests for judicial assistance in investigation and evidence collection raised by foreign courts, of which 19 were completed within 6 months, 16 were completed between 6 and 12 months, and 26 were completed beyond 12 months.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true.

August 14, 2024

Xiong (Carl) Li